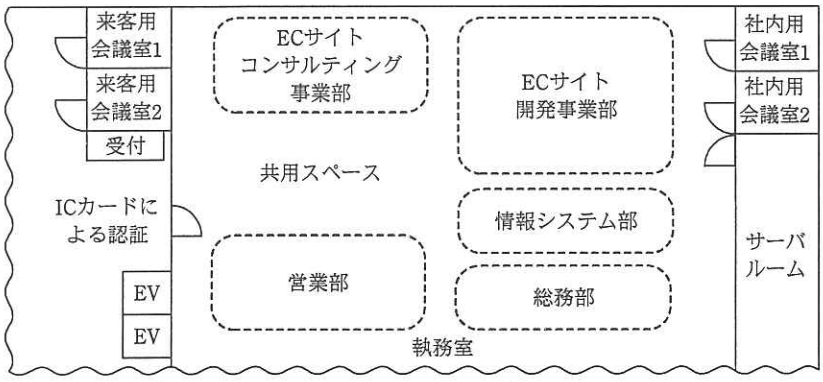
問2　無線LANの構築に関する次の記述を読んで，設問1～4に答えよ。

T社は，商品やサービスをインターネット上で販売するためのWebサイト（以下，ECサイトという）の開発，構築及び構築支援を主力事業とする企業であり，従業員数は150名である。T社には，ECサイト開発事業部，ECサイトコンサルティング事業部，情報システム部，営業部及び総務部の五つの部署がある。ECサイト開発事業部とECサイトコンサルティング事業部では，顧客から預かった機密資料や機密データを扱うケースが多い。

〔オフィス及びネットワークの構成〕

T社のオフィスは，都内のビルの1フロアにある。執務室では，座席を部署ごとに集めて配置し，その他に来客用の会議室を二つ，社内用の会議室を二つ用意している。T社のフロアのレイアウトの概要を図1に示す。



EV：エレベータ

注記　波線から左と下のレイアウトは省略

図1　T社のフロアのレイアウトの概要

各従業員には，ノートPC 1台と，入退室の認証に使用するICカードが貸与されている。入退室で通常使用する執務室のドアは1か所で，非接触型のICカードによって認証し，開錠を行っている。受付担当者は，来客があると，担当者を呼び出し，来客を来客用会議室に案内する。

T社のネットワーク構成の概要を図2に，社内サーバの機能一覧を表1に示す。

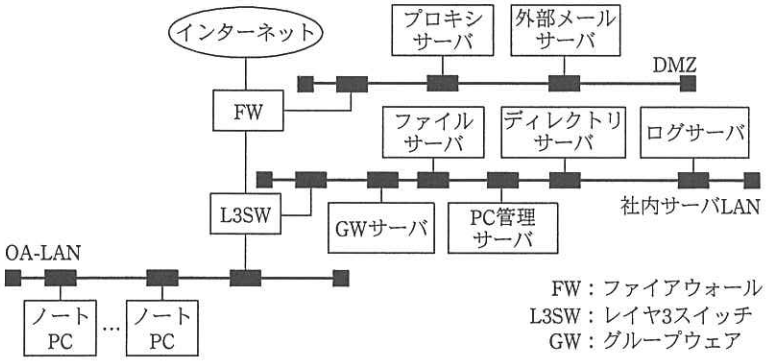


図２　Ｔ社のネットワーク構成の概要

表１　Ｔ社の社内サーバの機能一覧

項番	サーバ名	機能	備考
1	プロキシサーバ	・インターネット上の Web サイトにアクセスする際の利用者認証 ・ウイルスチェック ・URL フィルタリング	利用者 ID とパスワードによる利用者認証をディレクトリサーバで行う。認証にはベーシック認証を利用する。
2	外部メールサーバ	・インターネットから受信した T 社宛てのメールの，GW サーバへの中継 ・GW サーバから受信したメールの，インターネット上のメールサーバへの中継 ・添付ファイルのウイルスチェック ・スパムメールのフィルタリング	
3	ファイルサーバ	・ファイルの共有	次のフォルダが用意されている。 ・全従業員がアクセス可能な，全社共通のフォルダ ・各部の従業員だけがアクセス可能な，部ごとのフォルダ ノート PC とファイルサーバとの通信は暗号化されていない。
4	ディレクトリサーバ	・各利用者の氏名，所属（部署），メールアドレス及び認証情報の一元管理	
5	GW サーバ	・従業員及び社内リソースのスケジュール管理 ・Web メールサーバ	ブラウザから HTTP を利用してアクセスする。SSL は利用しない。 利用者 ID とパスワードによる利用者認証をディレクトリサーバで行う。
6	ログサーバ	・各サーバ上の OS，ソフトウェア及びネットワーク機器のログの収集・保管	ログ閲覧用の管理画面をもつ。
7	PC 管理サーバ	・ノート PC の OS のポリシ設定の強制適用 ・ノート PC にインストールされたソフトウェアのポリシ設定の強制適用	OA-LAN に接続されたノート PC を一元管理している。

ノート PC から社内サーバ及びインターネットへの通信の可否は，次のとおりである。

・社内サーバ LAN 上の全てのサーバとの通信は許可されている。

・インターネットへの通信は，FW で禁止されている。ただし，OA-LAN に接続されたノート PC 上のブラウザから，プロキシサーバを経由したインターネット上の Web サイトへのアクセスは許可されている。

L3SW 及び FW は必要最低限の通信だけを許可するよう設定されている。また，各サーバ及びネットワーク機器で取得したログは，ログサーバに転送し，保管している。

T 社の情報セキュリティ管理規程（以下，規程という）を図 3 に示す。

1.適用範囲
1-1. 本規程は，当社の従業員と，当社のシステム及びネットワークの利用者を対象とする。
（省略）
9. ネットワーク管理ルール
9-1. 社内ネットワークと社外ネットワークを接続する場合は，情報セキュリティ管理委員会の許可を得なくてはならない。
9-2. 当社のネットワークに接続する機器は，当社所有のものに限る。
（省略）
11. PC 管理ルール
11-1. 業務データはファイルサーバ上に保存することとし，PC への保存は禁止する。ただし，打合せを目的とした場合など，一時的な保存はその限りではない。
11-2. 個人所有の PC 及びその他の機器への社内情報の保管は禁止する。
11-3. 社内及び社外における次の行為は禁止する。
－当社所有の PC 及びその他の機器を業務以外で使用すること
（省略）
14. ログ管理ルール
14-1. 次のログを取得しなければならない。
－インターネットとの通信のログ
－情報共有サーバ（ファイル共有，スケジュール共有などを目的としたサーバ）へのアクセスのログ
14-2. 取得対象の各種ログにアクセスできるのは，その管理権限をもつ者に限定しなければならない。
14-3. 異常又は不正行為を発見するために，ログの確認を行わなければならない。
（省略）
20. 改定
20-1. 本規程の改定には，情報セキュリティ管理委員会の承認を必要とする。

図 3　T 社の規程（抜粋）

〔オフィス効率化委員会〕

T 社では，IT を活用した働きやすいオフィス作りを推進するために，オフィス効率

化委員会を月次で開いている。オフィス効率化委員会は，情報システム部の U 部長を委員長とし，メンバは各部から従業員 1 名を選出して構成しており，全社的にメリットがあると判断した要望について改善策を検討している。

最近，オフィス効率化委員会には次のような要望が多く寄せられている。

(1) EC サイト構築プロジェクトに関する要望

・EC サイト構築プロジェクトでは，EC サイトコンサルティング事業部と EC サイト開発事業部からメンバを集めて案件ごとにチームを編成する。ミーティングを行う機会が多いので，プロジェクトメンバの座席はまとめて配置してほしい。

(2) 会議室利用環境に関する要望

・社内用会議室と来客用会議室（以下，会議室という）には LAN がないので，会議中に資料が必要なときは，必要なファイルをあらかじめノート PC に保存した上で会議室内で参照・編集している。会議室から社内のファイルサーバにアクセスして，ファイルを参照・編集できるようにしてほしい。

・会議中に疑問点を調べるために，インターネット上の Web サイトを閲覧できるようにしてほしい。

U 部長は，次の改善策についてオフィス効率化委員会で検討することにした。

・EC サイト構築プロジェクトの効率を向上させるために，座席を柔軟に移動できるようにする。

・会議室利用環境の改善を行う。

オフィス効率化委員会では，“EC サイト構築プロジェクトの開始・終了時に，座席移動を行ったり，レイアウトを変更したりするとき，有線 LAN だと，その都度，LAN ケーブルを配線し直さなければならないので，社内関連部署に負荷が掛かる”という意見が出た。また，今後はスマートフォンを社内業務に導入していきたいという M 社長の意向があった。そうした背景を踏まえ，今回は無線 LAN の導入を検討することにした。対象エリアは執務室の一部と会議室とすることを決めた。U 部長は，情報システム部の C 君に，無線 LAN の方式を検討するように指示した。

〔無線 LAN 導入の検討〕

次は，C 君が無線 LAN 導入の検討結果を U 部長に報告したときの会話である。

U 部長：無線 LAN を導入する上で，盗聴・不正利用を防止する対策が必要になるが，それは当社の無線 LAN 上を流れる情報の特性や無線 LAN の利用可能エリアを考えると，どのようにすべきだろうか。

C 君　：まず，盗聴を防ぐためには①通信を暗号化する必要があります。そのための規格としては WPA2 を利用します。

U 部長：では，不正利用を防ぐにはどのようにすべきだろうか。

C 君　：無線 LAN を利用するノート PC の認証が必要だと考えています。その方式には，無線 LAN 用のアクセスポイント（以下，AP という）とノート PC との間で事前共有鍵を設定しておく方式と，動的に鍵を交換する [a] という方式があります。事前共有鍵を各従業員が設定する場合，②鍵を知る者の退職時などに必要なことがあります。一方，[a] を利用する場合は，認証サーバが必要ですが，ディレクトリサーバに認証サーバの機能をもたせることもできます。

U 部長：それなら，[a] を採用することにしよう。

C 君　：それから，より強固な認証を行うために，[a] の中でもクライアント証明書を用いる EAP-TLS を採用すべきです。

U 部長：なるほど。では EAP-TLS を採用しよう。クライアント証明書はどのように配布するのかな。

C 君　：クライアント証明書は，全て情報システム部がノート PC にインストールするのがよいと思います。

U 部長と C 君は，不正利用を防止する対策について更に検討を行った。次は，U 部長と C 君の会話である。

C 君　：無線 LAN の不正利用対策としては，他にも③ノート PC のネットワークインタフェースがもつ MAC アドレスによるフィルタリングや，AP が定期的に送信している [b] を停止する④SSID のステルス化，[c] 応答

の禁止がありますが，これらの対策も実施してはどうでしょうか。

U 部長：確かにそういう対策があるね。でも，それらの対策は，もし実施するとしても限定的な効果しかないことを踏まえておくべきだと思うよ。

〔会議室への無線 LAN 導入の検討〕

続いて，C 君は会議室への無線 LAN の導入について検討を進めた。まず，C 君は，1 台の AP では安定した通信を提供できないことから，執務室，社内用会議室，来客用会議室のそれぞれに AP を設置する方針とした。そして，次のようにすることにした。

- 会議室用の LAN（以下，会議室 LAN という）を L3SW 配下に新設し，そこに会議室用の AP（以下，会議室 LAN 用 AP という）を設置する。
- 執務室用の AP（以下，OA-LAN 用 AP という）は，OA-LAN 上に設置する。
- AP で取得するログは，その他のネットワーク機器と同様にログサーバへ転送する。
- 従業員が接続先の無線 LAN を識別できるように，執務室用の無線 LAN と会議室用の無線 LAN とで SSID を分ける。
- 接続先の無線 LAN を各従業員が設定できるように，ノート PC のネットワーク設定を変更する権限を，PC 管理サーバで各従業員に付与する。
- 会議室 LAN からアクセスできるサーバや機器は必要最小限に絞る方針とし，OA-LAN からアクセスできるサーバのうち，一部のサーバについては，会議室 LAN からのアクセスを禁止するよう L3SW を設定する。
- 会議室に導入する無線 LAN の暗号化方式や認証方式などは，執務室に導入予定の無線 LAN と同じにする。

C 君は，会議室への無線 LAN の導入についての検討内容を U 部長に報告した。

C 君　：以上のように検討しましたが，いかがでしょうか。

U 部長：会議室 LAN を新設するとなると，⑤アクセスコントロールについては，L3SW の設定だけでなく FW の設定も変更する必要があるね。

C 君　：承知しました。

C 君は U 部長の意見を踏まえ，無線 LAN の導入を進めることにした。

〔無線 LAN の導入〕

C 君は執務室と会議室への無線 LAN の導入を進め，無事導入を終えた。無線 LAN 導入後の T 社のネットワーク構成の概要を図 4 に，T 社のネットワーク接続ポリシを表 2 に示す。

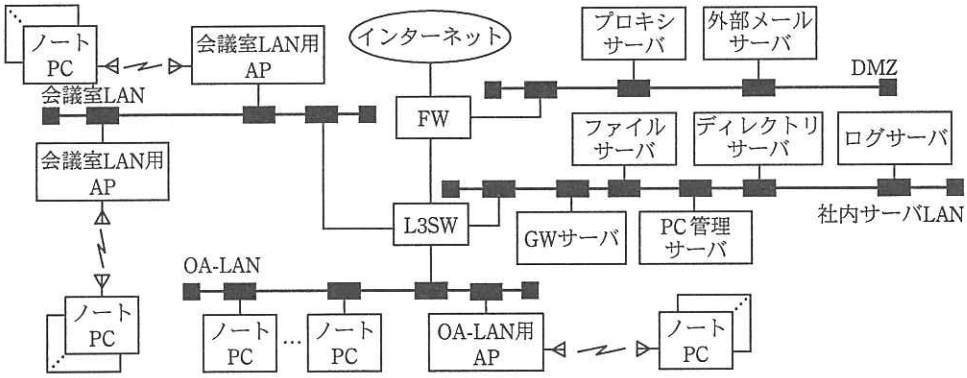


図 4　無線 LAN 導入後の T 社のネットワーク構成の概要

表 2　無線 LAN 導入後の T 社のネットワーク接続ポリシ

利用者＼接続先	OA-LAN（有線 LAN）	OA-LAN 用 AP	会議室 LAN 用 AP
EC サイトコンサルティング事業部員 EC サイト開発事業部員	接続不可	接続可	接続可
営業部員 情報システム部員 総務部員 役員	接続可	接続不可	接続可

〔内部監査での指摘〕

T 社では半年に一度，自社の情報セキュリティ上の問題点を洗い出すために内部監査を実施している。前回の内部監査以降に無線 LAN を導入したことで，オフィス環境が大きく変わっている。そこで，T 社では，今回の内部監査において無線 LAN の導入後のセキュリティ対策が適正かどうかを重点的に確認する方針とした。

内部監査の結果，2 件の問題が指摘された。次は，内部監査報告会での M 社長，U 部長，及び内部監査を担当した EC サイトコンサルティング事業部の K 部長の会話である。

K 部長：今回の内部監査の結果として 2 件の指摘事項を報告いたします。1 件目の重要度の高い指摘事項は，私物のデータ通信カード及び私物の携帯型無線 LAN

ルータを社内に持ち込んで，ノート PC をインターネットに直接接続している従業員がいるというものです。⑥セキュリティ対策のうち，幾つかは機能の実効性が損なわれてしまいます。この点については至急改善策を検討することを推奨します。

M 社長：それは問題だね。規程の周知徹底と技術的な対策とを併せて検討してほしい。技術的な対策としてはどのようなものが考えられるのだろうか。

U 部長：本指摘事項については，既存の仕組みを利用して対応可能であると考えています。ノート PC のログインアカウントを各従業員に割り当てていますが，⑦そのアカウントに応じて，OS のネットワーク設定のうち一部だけを許可し，それ以外を禁止します。

K 部長：2 件目の指摘事項は，来客用会議室内での従業員のノート PC の扱いが不適切な場合，⑧従業員以外の者が T 社のネットワークに不正にアクセス可能になる，というものです。

U 部長：本指摘事項については，新たなルールを規程に追加すればよいと考えています。

M 社長：了解した。では，進めてくれ。

内部監査報告会での指示を受け，情報システム部で改善を進めることにした。

〔来客用無線 LAN の準備〕

T 社では無線 LAN の利用が進み，“メンバが集まって座れるようになり，EC サイト構築プロジェクトメンバ間でのコミュニケーションがとりやすくなった”，“会議が効率よく行えるようになった”などの声がオフィス効率化委員会に寄せられるようになった。特に，会議中にインターネット上の Web サイトを閲覧できるようになったことは好評であった。

一方で，最近は来客が小型のノート PC やタブレット（以下，この二つをデバイスという）を持ち込むことが多く，プロジェクトによっては来客との会議でインターネット上の Web サイトを閲覧するケースも増えている。そのような来客用会議室の利用状況を踏まえて，来客用会議室を利用する来客にも無線 LAN を提供し，来客がインターネット上の Web サイトにアクセスできるようにしてほしいとの要望が出るようにな

った。オフィス効率化委員会では，来客用に無線 LAN を準備することにし，その検討をＣ君が行うことになった。

来客用に準備する無線 LAN について，Ｃ君は次のように検討結果をまとめた。

・LAN を新設して（以下，来客 LAN という），AP（以下，来客 LAN 用 AP という）を新たに設置する。

・無線 LAN を利用するデバイスの認証方式は，導入済の無線 LAN で採用している [a] では運用上の負荷が高いので，事前共有鍵方式を利用する。事前共有鍵は来客に設定してもらう。

・来客のデバイスから T 社内の各サーバには通信する必要がないことから，インターネット接続のための回線を新たに準備し，既存のネットワーク環境とは独立したネットワークを構築する。

・来客は，プロキシサーバを経由せずに直接インターネットにアクセスする。

・その際，通信のログは取得しない。

次は，Ｃ君の検討結果についてのＵ部長とＣ君の会話である。

Ｕ部長：来客用のネットワークであるので，当社のネットワークから独立させる方法もある。しかし，設置する AP のメンテナンスやシステムログの取扱いの観点からは，既存のネットワークに AP を設置した方がよいのではないだろうか。そうすることで，通信費用や機器購入のコストを抑えられるメリットもある。

Ｃ君　：そうですね。ネットワーク構成を見直します。

Ｕ部長：それから，現行の規程とネットワーク接続ポリシでは，来客が無線 LAN を利用することを想定していない。⑨来客への無線 LAN の提供によって，規程とネットワーク接続ポリシを見直す必要がありそうだね。ただし，セキュリティリスクが増大しないように，留意する必要がある。

Ｃ君　：承知しました。規程とネットワーク接続ポリシを見直します。

見直し後のＴ社のネットワーク構成の概要を図５に，見直し後のＴ社のネットワーク接続ポリシを表３に示す。

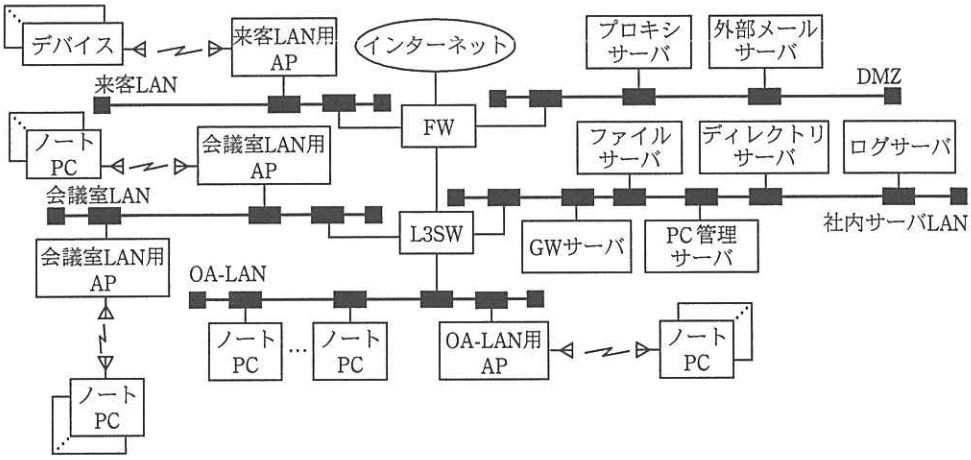


図５　見直し後のＴ社のネットワーク構成の概要

表３　見直し後のＴ社のネットワーク接続ポリシ

利用者＼接続先	OA-LAN（有線 LAN）	OA-LAN 用 AP	会議室 LAN 用 AP	来客 LAN 用 AP
EC サイトコンサルティング事業部員 EC サイト開発事業部員	接続不可	接続可	接続可	接続不可
営業部員 情報システム部員 総務部員 役員	接続可	接続不可	接続可	接続不可
来客	接続不可	接続不可	接続不可	接続可

オフィス効率化委員会の検討結果を受けて，情報システム部は，来客 LAN の構築を行った。

設問１　〔無線 LAN 導入の検討〕について，(1)～(3)に答えよ。

(1)　本文中の［ a ］～［ c ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　802.11i　　イ　802.1X　　ウ　ALL　　エ　ANY プローブ

オ　PSK　　カ　SHA-1　　キ　SHA-2　　ク　WPS

ケ　ビーコン

(2)　本文中の下線①について，C 君が，通信を暗号化する必要があると判断した理由を，T 社の無線 LAN 上を流れる情報の特性の観点，及び無線 LAN の利用

可能なエリアの観点から，それぞれ30字以内で述べよ。

(3) 本文中の下線②について，C君が必要なこととしている内容を10字以内で答えよ。

設問2 無線LAN環境におけるセキュリティ対策について，(1)，(2)に答えよ。

(1) 本文中の下線③及び下線④の対策は，必ずしも効果が得られない。その理由を，それぞれ20字以内で述べよ。

(2) 本文中の下線⑤について，FWの設定はどのように変更すべきか。30字以内で述べよ。

設問3 〔内部監査での指摘〕について，(1)～(3)に答えよ。

(1) 本文中の下線⑥について，ノートPCを直接インターネットに接続する場合に，実効性が損なわれてしまう機能とは何か。二つ挙げ，それぞれ10字以内で答えよ。

(2) 本文中の下線⑦について，従業員のアカウントに応じて許可するOSのネットワーク設定とは何か。ネットワーク接続ポリシを踏まえ，ECサイトコンサルティング事業部員及びECサイト開発事業部員のアカウントの場合と，それ以外の場合の二つに分けて，それぞれ45字以内で述べよ。

(3) 本文中の下線⑧の状況を招くノートPCの不適切な扱いとは何か。20字以内で述べよ。

設問4 〔来客用無線LANの準備〕について，(1)～(3)に答えよ。

(1) 本文中の下線⑨について，規程のうち，見直す必要があるとしている項目を二つ挙げ，図3中の番号で答えよ。また，各項目について，来客の無線LAN利用が抵触する内容を，35字以内で述べよ。

(2) 無線LANのデバイスの認証方式を検討する上でC君が考慮した，運用上の負荷とは何か。30字以内で述べよ。

(3) 来客がインターネット上のWebサイトにアクセスできるようにするために，FWに追加すべき通信許可ルールを，送信元ネットワーク，宛先ネットワーク，通信プロトコルの三つの組で答えよ。

なお，送信元ネットワーク，宛先ネットワークについては図5中の字句を用いてそれぞれ一つ答え，通信プロトコルについては二つ答えよ。